Image Forgery Detection Comparison between MobileNetV2 and VGG16 Convolutional Neural Networks

by

Aritra Nandy
16101315
Md. Mustakim Hasan
16110018
Abu Bakar Md Sayad
15301115
Imteenan Akhter Khan
15301008
Amina Azad Anindita
13310004

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
BRAC University
October 2020

Declaration

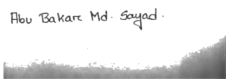
It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I/We have acknowledged all main sources of help.

Student's Full Name & Signature:

Aritra Nandy
16101315

Md. Mustakim Hasan
16110018



Abu Bakar Md Sayad
15301115

Imteenan Akhter Khan
15301008

Amina Azad Anindita
13310004

Approval

The thesis/project titled "Image Forgery Detection Comparison between MobileNetV2 and VGG16 Convolutional Neural Networks" submitted by

1. Aritra Nandy - 16101315

2. Md. Mustakim Hasan - 16110018

3. Abu Bakar Md Sayad - 15301115

4. Imteenan Akhter Khan - 15301008

5. Amina Azad Anindita - 13310004

In Summer, 2020 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on October 9, 2020.

Examining Committee:

Supervisor:
(Member)

Dr. Jia Uddin
Associate Professor (Research Track)
Technology Studies Department, Endicott College, Woosong University
Daejeon, South Korea
Associate Professor (On Leave)
Department Of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Dr. Md Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Prof. Mahbub Majumdar
Chairperson
Dept. of Computer Science & Engineering
Brac University

Prof. Mahbubul Alam Majumdar
Professor
Department of Computer Science and Engineering
Brac University

Abstract

As there are an immense scope of useful assets to alter images now, the requirement for confirming the authenticity of images is more necessary than any time in recent memory. While forgery techniques are progressively getting better that even human perception appears quite difficult to perceive these changes, regular algorithms, which attempt to identify altering patterns, frequently pre-define suppositions that restrict the extent of issue. In this manner, such strategies fail to detect forgery strategies in computer programs. Inside the following publication, we initiate structure which uses Machine Learning methods to distinguish forged photos. Consequently, the MobileNetV2 network in [40] is altered with the goal that it very well may be well equipped to the goal of image forgery identification. It is contended by the rest spatial measurements of initial layers, the system is probably going to learn prominent highlights in these layers, and afterward succeeding layers are to extract these prominent highlights and coming to a conclusion determining an image is tampered. Furthermore, by our efforts we additionally lead an extensive examination to demonstrate those contentions. Exploratory outcomes show that this architecture-modified system accomplishes an amazing accuracy of 93.15%, which outperforms VGG16 neural network on which the previously defined system depends with a margin of healthy amount up to 10.05%.

Keywords: *picture tampering;machine learning;MobileNetV2; VGG16 neural architecture; Copy-move forgery; Splicing forgery; neural networks*

Dedication

Firstly, this research work is dedicated to our parents, without whom we would not have been here today. Through their sacrifices and meaningful lessons about life, they made us work hard and dedicate ourselves to achieve ultimate goals.

It is also dedicated to our beloved supervisor, who believed in us throughout this journey and always motivated us to keep looking for a solution. Without his guidelines and teachings, this would not have been possible.

Lastly, we dedicate this work towards BRAC UNIVERSITY, which as a standout institution of Bangladesh, is continuously giving support to its students for becoming a global citizen. Because of this platform, we were able to share the knowledge we gathered over time.

Acknowledgement

First person who should be mentioned is the most important person who kept supporting us for this research and he is our honorable thesis supervisor Dr. Jia Uddin who acted not only as our supervisor but also our guardian. His continuous Support took us this far. Secondly we would love to thank other faculty members and so many senior brothers and sisters and friends for guiding us through the right path and providing us with unfailing support and continuous encouragement through the process of researching and writing this paper. This successful journey would not have been possible without them. Thank you.

Table of Contents

List of Figures

Chapter 1

Introduction

The identification of the existence of tampered images is of great importance in digital forensics.The problem with the current literature is that most of them define those features in images that are manipulated by a specific form of manipulation (such as copy-moving, splicing, etc.). It means the system does not operate consistently through multiple forms of manipulation. Furthermore, much of the research targets only JPEG images in terms of tampered area localization due to the manipulation of double compression artifacts left during the manipulated image re-compression. By fact, however, digital forensics tools should not be limited to any photo format, and should also be able to locate the region of the changed image. Inside the following publication we propose a two-stage deep learning systaem with the help of MobileNetV2 and VGG16 neural system for learning features to detect manipulated images in various image formats.Resulting in good showing in classification, regression, anomaly detection, time-series pattern complications with distinct features, CNN processes to obvious security issues are a common theme in research field in these times. Conventional machine learning algorithms such as random, vector supporting machines are not suitable when it comes to photos, presentation, signal waves, text and so on problems compared to deep learning techniques. Machine learning algorithms can extract useful features on their own, whereas conventional ML algorithms need manual feature engineering. So in following publication we introduce a two step process for image forgery detection using CNN. By comparing the results provided by MobileNetV2 and VGG16 we reach to a conclusion which states that MobileNetV2 provides superior accuracy and does so with less computation time than it's counterpart VGG16 neural network.

1.1 Motivation

With the rise of social media and online platforms, carefully curated misinformation has started dominating the global scene, whether it is fake news, fake scandals or the use of powerful editing software to create confusing propaganda, fake images play an important part in inciting people's emotions to make them take action!
We too have unknowingly fallen victim to such images and hence, want to reduce, if not eradicate the use of fake images around the internet by detecting tampered images using CNN.

1.2 Thesis Objective

1. Designing a model that will help law enforcement in detecting forged evidences in crime forensics
2. Recover lost evidences
3. Helping with identification in various fields such as various examinations, surveillance inspection, forensic analysis and biomedical imaging
4. Minimizing cyber crimes to some extent
5. Assisting the mass public in distinguishing authentic and forged images.
6. Stopping people from getting misguided from altered images on the internet.

1.3 Thesis Orientation

The following thesis is presented as such :-

1. Chapter 2 discuss image forgery detection and the ways it is done in details
2. Chapter 3 includes the necessary literature review with references
3. Chapter 4 presents the methodology used in the implementation
4. Chapter 5 demonstrates the analysis and the comparison between the results generated by the two neural networks
5. Chapter 6 describes future works and conclusion

Chapter 2

Image Forgery

2.1 Image Forgery

Forgeries are an age old concept. In the past it was restricted to art and literature be that as it may, didn't influence the general population. These times, for the reason of the progression of digital picture creation software and editing tools, a picture can be handily manipulated and adjusted . It is hard for people to recognize straight forward if the photo in question is unique or tampered. There is a sudden increment in surgically conducted tamperings in traditional media and on the world wide web .This pattern demonstrates real weaknesses and diminishes the believability of digital pictures. In this way, organizing processes to confirm the authenticity and legitimacy of the digital photos is very significant, particularly thinking about that the photos are introduced as artifacts in an official courtroom, as news items, as a sample clinical records, or as financial archives. In this sense, photo forgery detection is one very much importantly needed aspirations of image forensics.Image Forgery implies control of the digital picture to disguise some significant or helpful data of the picture. There are situations when it is hard to recognize the tampered area from the original picture. The recognition of a forged picture is driven by the need of realness and to keep up integrity of the picture.
[12]

2.2 Copy Move Forgery

Analysts[20]-[22] usually use strong coordinating techniques, such as SIFT[23] and SURF[24], to discern the duplicate copy movement technique for manipulation. The reason for this use is the ability of these matching techniques to transition, scale, and rotate. So, despite the fact that the forged objects are special in comparison to the sources, they are still identified. Nonetheless, these kinds of approaches aim not to proceed as precisely true to form, tiny items or papers that contain less example structure information. This can be explained by the fact that, before performing a matching procedure, If anyone wants to extract features on which the object of the data depends they must use SIFT or SURF. In this way, copies that contain less example structure information are likely to be skipped by the matching stage. There is also a section of the method that isolates a picture into blocks, at which point a transform (Discrete Cosine Shift (DCT)[25]-[27], Discrete Wavelet Transform (DWT)[28], and Zernike moment[29]) is performed on these fragments to withdraw

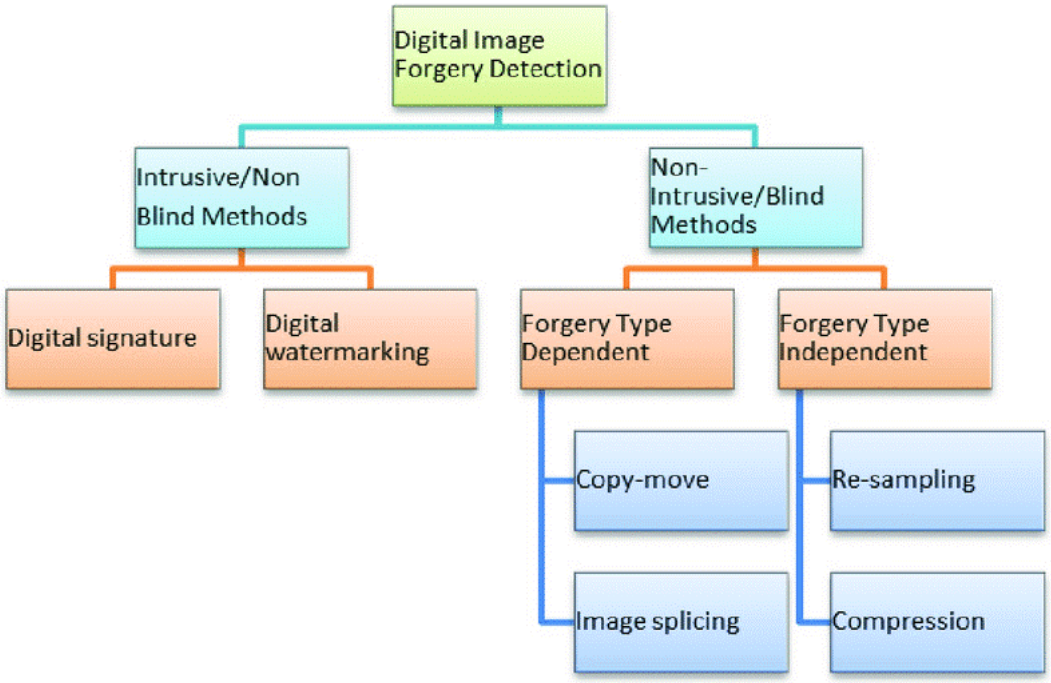


Figure 2.1: Classification of Image Forgery

significant characteristics that lead to a matching level. Even more importantly, function vectors are evaluated as separate sets in the matching process.If the score of similarity is lower than a limit initialized before, a pair is assumed to be paired. The identity is a way which uncovers how two feature vectors in a capacity presented to be comparable. The calculation is usually the notable Euclidean distance..

Figure 2.2: Example of a Copy move forgery

2.2.1 Splicing Forgery

In fact, the forgery of splicing is both more normal and intricate than the strategy of copy movement, since joined items originate within various origins. Zhang et al . suggested a differentiation program in [30] to identify these performed splicing.

DFT, and Image Quality Metrics have been performed an element of size 200 perform training on a CNN for all the more simple, moment-based features extricated using DWT what's more. At that point, the CNN was to organize fragments of a photo in to two types, positive and negative in particular. In[31], however, the authors addressed the use of saliency detection as an aid to detect image splicing. They viewed protruding items as unmodified, so they could make sense of copied areas by eliminating a protruding map. Pan et al.[32] used a system in an alternative branch that used noise models to distinguish forged areas.The inserted photo was solidly switched to the DCT domain. A model was developed from that point forward to gauge the noise change in the non-covering areas of the picture. Finally, a clustering stage was intended to segregate forged and genuine patches using the K-mean algorithm. In addition, Fridrich and Kodovsk [33] continued to investigate how noise estimation is utilized in digital image stegana.They depicted a technique in digital images to identify steganography. Using direct and nonlinear high-pass filters, the noise residuals of the input image are measured. At that point, the joint dissemination of these noise residuals was carried out by a different number of models. To frame a rich model for identifying steganography, these models were gathered.

Figure 2.3: Example of Splicing image Forgery

2.2.2 Deep Learning Based Methods

Since traditional strategies regularly assume a few constraints that limit the nature of the problem they are solving, in general circumstances, such techniques may not be implemented. In [34], a hybrid method was planned by Goh and Thing to separate forged photographs. In order to separate component vectors a rundown of methods was considered. All of these features were gathered and an optimal arrangement of features was selected using a transformative Memetic algorithm. In addition , the authors proceeded to apply the Genetic algorithm to streamline a classifier outfit to make a final option. Despite the fact that the outcome provided encouragement, the process still relied on manually conducted highlights and prompted complex calculation by the troupe of different classifiers. It has occur ed world renowned works using Machine Learning to recognize tampered photos due to hardware advancement (e.g.,(GPU), (TPU)).For overlapping blocks within an image, Zhang et al.[35] performed the DWT to remove feature vectors of dimension 300. A while later , in order to organize the block was tempered, these feature vectors were placed

into a CNN. In addition, Rao et al.[36] suggested a 10-layer Convolutional Neural Network (CNN) model, an SVM classifier, and a highlight combination to identify image level forgery. They looked at the efficiency of initialization strategies between Xavier and SRM[30] and discovered certain evidences that latter CNN was developed and training was completed more accurately. Authors in [37] used resampling functionality and deep learning instead of using CNN. There, they suggested two strategies. Re-sampling features of covered divisions taken from in the primary process, and these features are modified using Radon transform.

Chapter 3

Literature Review

Forgery detection techniques are required to verify the authenticity of digital images. In 2018, A.Doegar, M.Dutta and G.Kumar [1] proposed a method for image forgery detection using Pre-trained AlexNet Model. Image forgery detection is an approach designed to identify and locate the forged part from a manipulated image. To find distortion or tampering in the original image, it takes a sufficient number of features to identify the given image as either a forged or non-forged one. The deep features of this pre-trained AlexNet model based on convolutional neural networks (CNN) have been used that are robust and powerful compared to the current state-of - the-art approaches to the publicly accessible MICC-F220 benchmark dataset. The result of the experiment shows that the proposed method with the Support Vector Machine (SVM) classifier using a pre-trained AlexNet model based deep features has achieved 93.94 per cent accuracy.

Deep Learning approach has proved to be quite effective in detection of image forgery. So in 2016, Y.Zhang, J.Goh, L.Win and V.Thing [2] came up with a forgery detection method in the digital forensics field. The identification of the existence of altered images is of great importance in digital forensics. The problem with the current literature is that the big ones describe those features in images that are manipulated by a specific form of manipulation (such as copy-moving, splicing, etc.). This means the system does not operate consistently through multiple methods of tampering. In addition, much of the research targets only JPEG images in terms of tampered area position due to the manipulation of double compression artifacts left during the manipulated image re-compression. In fact, however, digital forensics tools should not be limited to any image format, and should also be able to locate the region of the changed image. In this paper, they have proposed a two-stage, deep learning method for learning features to detect manipulated images in various image formats. For through indi-vidual patch we use a Stacked Autoencoder model to learn the complex function. They incorporated the contextual details of each patch for the second level, so that the identification can be carried out more accurately. In their experiments, they were able to achieve a cumulative manipulated area localization accuracy of 91.09 percent for both JPEG and TIFF images from CASIA dataset, with a 4.31 percent fall-out and 57.67 percent accuracy respectively.

Median Filtering Forensics is an integral part of image forgery detection in digital forensics. In 2015 J.Chen, X.Kang, Y.Liu and Z.J.Wang [3] proposed a method.

Median filtering detection has recently drawn much attention in image editing and image anti-forensic techniques. Cur-rent image median filtering forensics algorithms mainly extract features manually. To deal with the challenge of detecting median filtering from small-size and compressed image blocks, by taking into account the properties of median filtering, they proposed a median filtering detection method based on convolutional neural net-works , which can automatically learn and obtain features directly from the image.

Another method for image forgery detection can be using error level analysis and deep learning. In 2019, I.B.K.Sudiatmika, F.Rahman and T.Suyoto [4] came up with a method. In the virtual world of social media, several photos are spread out. With the many editing tools that make so there's no question that there are a lot of fake images. By using Error Level Analysis to forensic the image to determine the compression ratio between the original image and the fake image, since the original image compression and fake images are different. Besides knowing whether the image is true or false, the metadata of the image may be examined but the likelihood of metadata may be modified. In this case, the authors apply Deep Learning to recognize images of manipulations through a fake image dataset and original images via Error Level Analysis on each image, and to support parameters for error rate analysis.

Copy-Move is a commonly used operation of image forgery. In 2019, Y.Abdalla, M.T.Iqbal and M.Shehata [5] came up with an image forgery detection model using a generative adversarial network and CNN. The issue of faked images has become a global phenomenon which mainly spreads via social media. New technologies have provided both the means and support for this trend, but they also make it possible to resolve a targeted response. One approach to this is deep convolutional learning algorithms. These have been shown to be highly successful in resolving image forgery resulting from adversarial generative networks (GANs). In this sort of algorithm, the image is changed in such a way that it appears to be identical with the original image and is almost undetectable as a forgery to the unassisted human eye. The paper uses a fusion processing model comprising a deep convolutional model and an adversarial model to examine the detection of copy-move forges using four datasets. Their findings indicate that the deep learning CNN and discriminator forgery detectors have a significantly high detection accuracy efficiency (95 per cent). Thus, the best method seems to be an end-to-end trainable deep-neural network approach to forgery detection. The network is based on two-branch architecture and a fusion module.

In 2018, M.T.H.Majumder and A.B.M.Alim Islam [7] proposed a method of deep learning approach using CNN. In modern times social media has become a part and parcel of people's lives. It has become much easier to create fake images because of the high availability of cameras and the inclusion of numerous image editing devices in mobiles. These misleading and distorted photos can and will be used in dirty political actions to smear the reputation of famous figures. The problem of identifying and finding such images is known as the detection of image forgery.Deep learning without manual feature engineering approaches is very difficult to implement because of how small the edited regions are compared to the full size of the image.

In 2019, X.Wang, H.Wang, S.Niu and J.Zhang [8] came up with a method of image forgery detection using improved mask regional convolutional neural networks. Work on forgery detection and localization in digital forensics is important, and has recently attracted growing interest. Traditional approaches are often based on handcrafted or shallow-learning features, but they have limited ability to explain and high computational costs. Recently, deep neural networks have demonstrated the ability to derive complex statistical features from high-dimensional inputs, and to learn their hierarchical representations effectively. In order to capture more discriminative features between manipulated and non-tampered regions, they are proposing an improved regional convolutional neural network mask (Mask R-CNN) which in this paper adds a Sobel filter to the mask branch of Mask R-CNN. The Sobel filter serves as an adjunct function to enable projected masks to have identical gradients of image to the ground truth mask. Two different forms of image manipulations can be identified by the overall network, including copy-move and splicing.

In majority of the cases copy-move image forgery technique is used to alter the digital image, in which a portion of the image is copied and pasted somewhere else in the same image with the purpose to cover an important image characteristic. In 2016, Y.Rao and J.Ni [9] proposed a method to detect a copy move forgery and image splicing. In this paper they have presented a new method of detection of image forgery based on deep learning technique, which uses a convolutional neural network (CNN) to automatically learn hierarchical representations from the RGB color images data.The proposed CNN is primarily intended for use for image splicing and copy-move detection.Instead of a random strategy, the weights at the first layer of our network are initialized with the simple high-pass filter set used in the measurement of residual maps in spatial rich model (SRM), which serves as a regularizer to effectively suppress the effect of image contents and capture the subtle artifacts introduced by the manipulating operations. As a patch descriptor, the pre-trained CNN is used to extract dense features from the test images, and a feature fusion technique is then explored to obtain the final discriminative features for classification with SVM.

Copy-Move in an image might be done to duplicate something or to hide an undesirable region. In 2016, P.Rota, E.Sangineto, V.Conotter and C.Pramderdorfer [10] came up with a deep learning approach in the field of forensics analysis. The widespread use of the Internet, combined with the emergence of ever more effective technology, has made digital images the primary source of visual knowledge in society today. However, due to the inexpensive powerful graphics editing software that can easily modify the original content, their reliability as a true rep-resentation of truth can not be taken for granted, leaving no visible evidence of any alteration on the image making them potentially dangerous. This motivates the creation of technical solutions capable of detecting media manipulations without prior knowledge or additional details concerning the image provided. At the same time, the immense amount of data available has also led to considerable developments in data-hungry learning models, which have already proven popular in image classification in the last few years. Through this thesis they suggested a deep learning method for the classification of manipulated images. This is the first attempt to use the deep learn-

ing model in a forensic picture scenario, to their best knowledge. In particular, they are proposing a new blind deep learning approach based on Convolutional Neural Networks (CNN), able to learn from manipulated images of invisible discriminative objects that can be exploited to automatically differentiate between fake and authentic photos. Not only does the proposed method detect faked images, it can also be generalized to localize the regions inside the image that have been corrupted. This approach outperforms the state-of - the-art on the CASIA TIDE v2.0 dataset in terms of precision.

In 2018, R.R.K and M.Wilsey [11] used a pre-trained convolutional neural network as a feature extractor for image splicing detection. Recent years have seen the detection of image forgery emerge as an important research field. In this research, they concentrated on detecting people-involving image forgeries, and used pre-trained Convolutional Neural Networks (CNNs) to extract features from the illuminating image maps. The extracted functions are then fed for classification to a Support Vector Machine (SVM). The experiments are conducted on DSO-1 and DSI-1, two different publicly accessible datasets which deal with people's image forgeries. They evaluated and compared the performance as feature extractors of five pre-trained CNNs, such as AlexNet, VGG-16, VGG-19, GoogLeNet and Inception-v3. The result shows that by using Alexnet, VGG-19, GoogLeNet and Inception-v3, the proposed method gives a 97.5 percent detection accuracy on the DSO-1 dataset. Using Alexnet as a function extractor, a cross-dataset detection accuracy of 84 per cent is achieved on the DSI-1 dataset.

Chapter 4

Methodology

In this paper, in both copy-move and splicing situations, we present a Deep Learning method for separating forged images. The input picture is divided into overlapping patches to begin with. Using MobilenetV2[40], these patches are extricated (logit) functions. As a result of its lightweight configuration, its architecture is adopted for the implementation of a powerful deep CNN on: the quantity of parameters and add-multiply are typically tiny, compared with another. Finally, to determine if the input image is manipulated, a processing stage is to amass extracted features.We argue, however,that phase 2 in early layers can prompt free patch information details. We are altering the MobilenetV2 architecture along these lines to preserve the spatial structure in bottom layers. Therefore, on the CASIA2 dataset[39], our model acquires a fair precision of 93.15 percent.

4.1 Dataset

The terms used will be made clear prior to moving into the dataset summary.

1. Fake Image: Two mostly used tampering works, namely: copying / pasting and splicing of images, a photo is manipulated / doctored.
2. Pristine Image: A photo where there is no forgery, only the necessary editing to bring to authentic size is done.
3. Image Splicing:The splicing operations would blend the photos of humans, add windows to homes, add various objects to parking lots, etc. Sections of the corresponding copy / pasting operations can also be used in the spliced images. An image called a "host" is the image that receives a spliced component. The bits spliced together with the host image are called "aliens.""

You will find the complete dataset for the first and second phases here [13]. We're going to use a train set for this project. It contains two directories, one with not real photos and their accompanying , and the latter with photos that are pristine.A bw image that depicts the cut ted region of the false photo is a false image mask. In the mask, the black pixels indicate the region in which the source image was distorted in order to get the image created, specifically representing the spliced field.

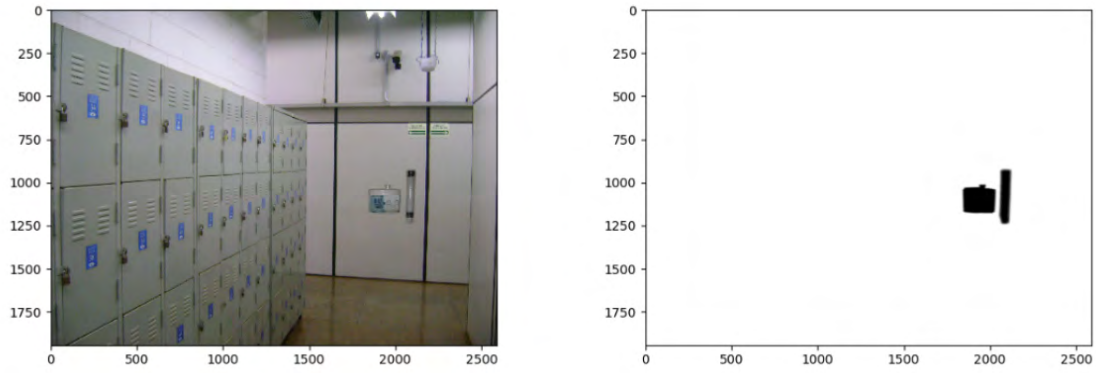


Figure 4.1: Demonstration of a fake photo and it's complimentary masks

1050 pristine images and 450 false ones are included in the dataset. In general, colour photos are 3 channel images, one channel for RGB color , but sometimes another channel for Y may be present. In our dataset, the images are a mix of 1, 3 and 4 channel images.
In order to generate robust solutions to such noise, these images were implemented on purpose. Therefore, many of them were used while others were discarded as noise. They still had no valuable knowledge when they came to four pictures on networks. They were pixel-loaded grids of 0 values. So, after cleaning, our pristine data collection included about 1000 RGB pictures. False photos are a mixture of images on 3 and 4 channels, but none of them are noisy. A mixture of images from 1, 3, and 4 sources are the corresponding masks. The extraction of the feature we will use involves data from only one source of the mask. So, there are 450 fakes in our fake corpus of images. We conduct spliting training to keep 10 percent of 1500 images .

4.2 VGG16 Convolutional Network for Classification and Detection

Here network is trained in such a way, the input image in the Cov1 layer has a fixed size of 224x224 RGB images. The image is passed through multiple filtered convolutional layers with a very small susceptible field of 3x3 (smallest size to figure out the notion of up/down, left/right. center). It also uses 1x1 convolution filters in one of its features which can be observed as a linear transformation followed by non-linearity of the input channels. Spatial pooling is performed by five max-pooling layers (2x2 pixel window, stride 2) which follows some convolution layers. Three Fully Connected layers follow a stack of convolution layers where the first two are composed with 4096 channels in each and the third contains 1000 channels (one for each class) as it performs 1000-way ILSVRC classification. The final layer is a soft-max layer. The Fully connected layers are configured to perform the same in all networks. The hidden layers are featured with Rectification non- linearity also no networks (except one) contain Local Response

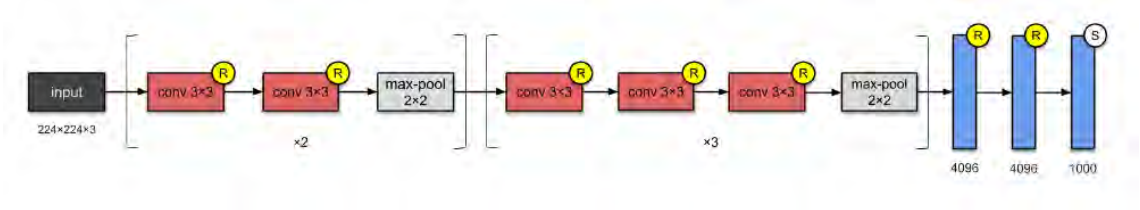


Figure 4.2: VGG 16 Neural Architecture

4.3 Feature Extraction on train set

The dataset cannot inclined to train. Dataset must be configured in such a way to tailor our needs i.e. the recognizing by forging operations of pixel-level abnormalities. To create relevant images from the data given, we created the following process, taking ideas from here[9]. In case of counterfeit image, we have a complimentary mask. Utilizing the mask to figure out the tampered photo along the periphery of the spliced pixel in such a way that both the forged and unforged parts of the image ensure a contribution of at least 25 percent. The distinctive limits that would only be present in false images would be present in these proofs. The CNN we're creating is about learning from those constraints. Since the same information is present in all 3 mask channels (falsified portion), we only need 1 channel to obtain samples. To make peripheries even clearer, after using a Gaussian filter, the bw images were changed to binary using Otsu 's threshold.

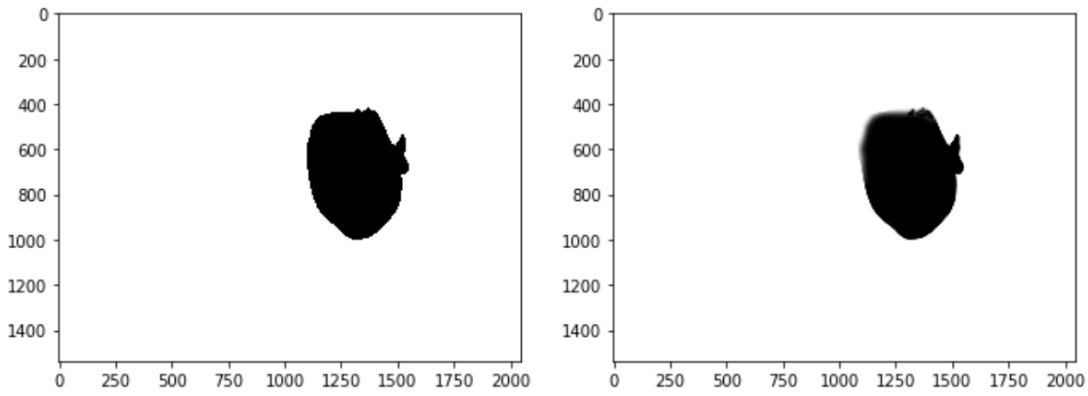


Figure 4.3: Peripheries are more prominent is a binary mask

We received 175,119 64x64 patches from fake photos after sampling. We sampled approximately the same amount from the authentic images to produce 0 labeled (pristine) patches.
We now accomplish a huge dataset of images with good quality feedback. It's time to experiment with various models.

4.4 Working Mechanism of CNN

CNN, which stands for Convolutional Neural Networking, is a type of artificial neural network that called convolutional layers has hidden layers. CNN also contains other non-convolutionary structures.Convolutional layers take inputs, use filters to identify patterns, then transform the inputs and send them to the next layer.
The role the convolutionary layers perform can be divided into 3 steps:

1. Convolution: Merge input sets to construct a map of the function.
2. Pooling: Reduces the dimensionality of a function map which results in a drastic reduction of the input spatial dimension.
3. Non-Linearity: Passes via relu-activation function the product of the convolution process.

Growing filter is tasked with defining a single feature of an input. The deeper the network goes, the more such filters become sophisticated.

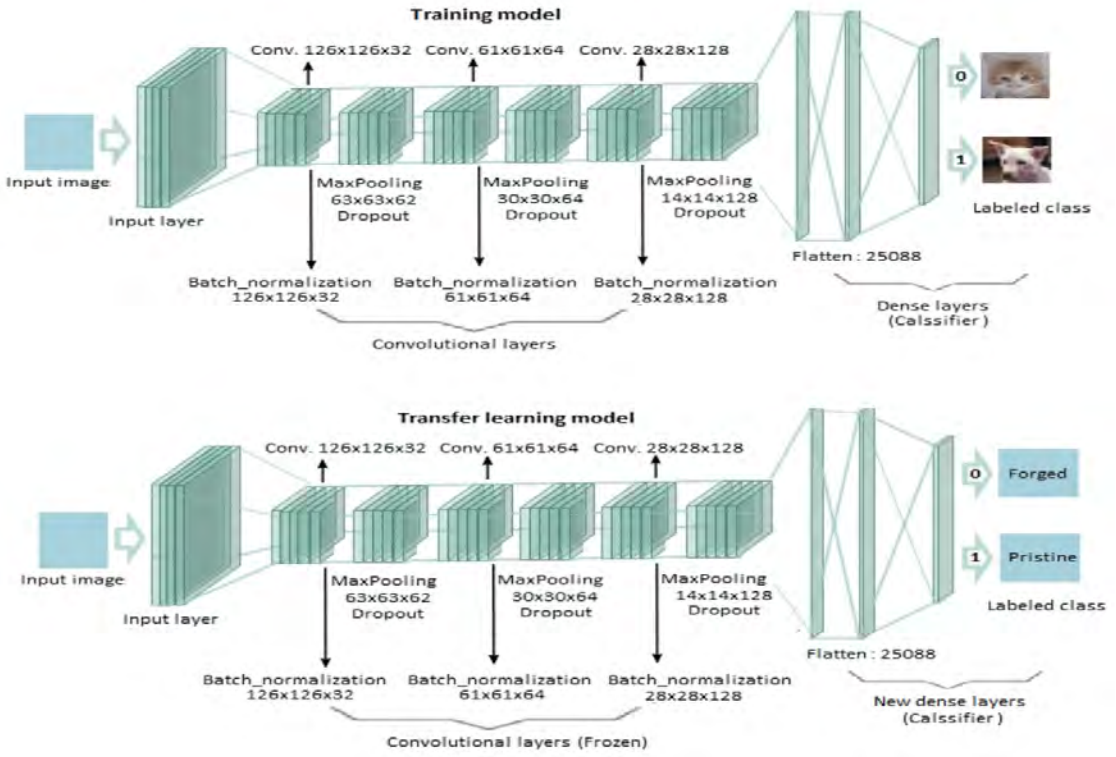


Figure 4.4: Block Diagram of CNN taken from European journal of Electrical Engineering and Computer Science[15]

4.5 Forgery Detection Algorithm

We have used machine learning procedures to classify images into two categories in the following writing to solve splicing 1 detection: original and distortion included.

The method uses examining the photo in a slider and classifying each photo pixel according to the location of the window. This method without prior knowledge of the extraction process, to create discriminating functions directly on the basis of the data. We use CNN in this paper, which have scored very good scores in many applications of computer science in recent years, such as image detection , object recognition , image segmentation, face recognition, and many others.However current dataset are not suitable enough to train complex CNN models such as VGG-16[14] (Figure 4.5).

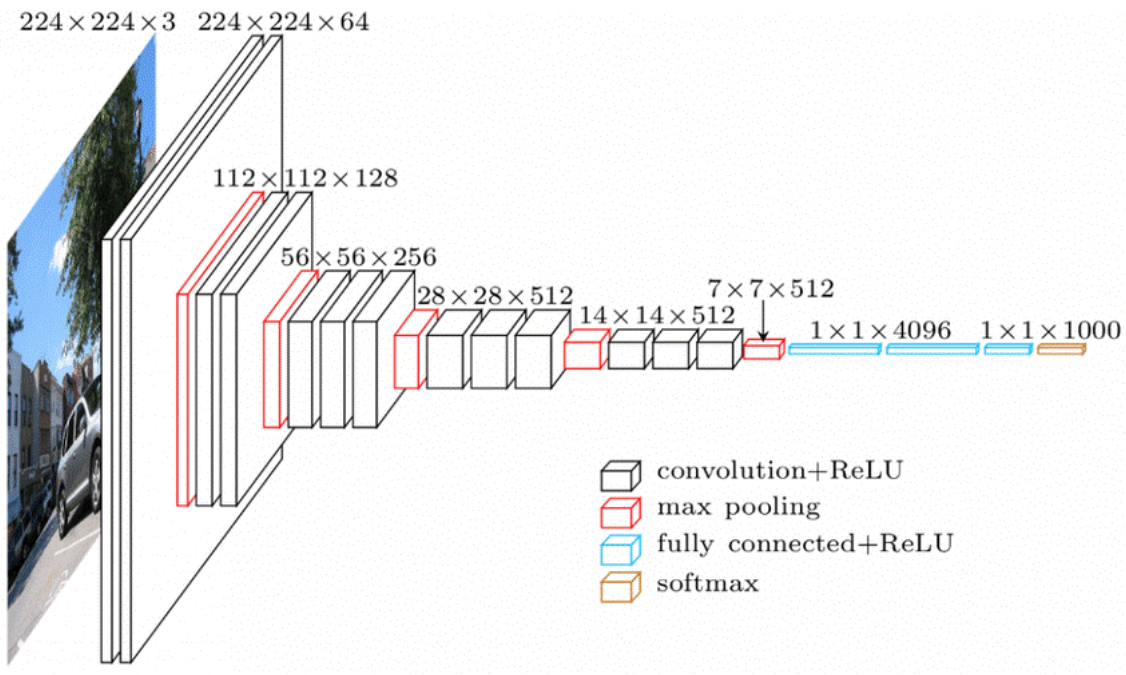


Figure 4.5: VGG-16 Model[14]

For VGG16, the training precision seems to level off after one epoch, with the approval accuracy remaining steady for the whole fitting time frame. Upon examining web research highlights an inferior streamlining agent and learning rate. However in the wake of altering the learning rate to various qualities, the precision was identical.

4.6 MobileNetV2 modification

In[40], on the ImageNet dataset, developers trained the network, by resizing the photos in 224 before putting them through the CNN. The first MobileNetV2 model appeared in Table I.In particular, s means the phase in a bottleneck of the first convolutionary layer. The move lessen spatial aspect of feature tensors that allows higher features from past layers to be coordinated by the network. The output tensor (previously the GAP) has a dimension 32 times smaller than the input image in the original form. Nonetheless, the patches removed from the images in our dataset have a dimension of 64 , the first model is not, at this stage, sufficient as a result of the large subsampling of 1/32. Therefore, bottom layers need to be wide to capture primary information for convolutionary filters in a transparent and high-resolution

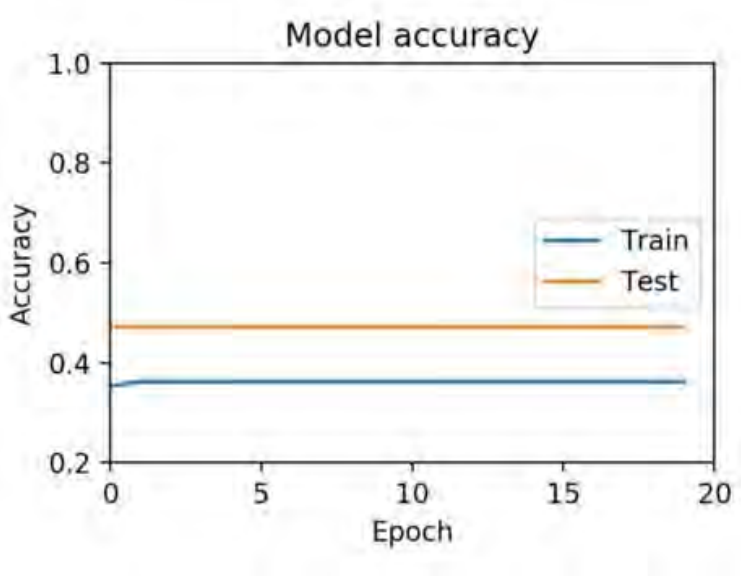


Figure 4.6: Accuracy provided by VGG16

way.We change the original MobileNetV2 architecture based on the above claims in such a way that the early layer dimension is reasonably high resolution. We change the original MobileNetV2 architecture based on the above claims in such a way that the early layer dimension is reasonably high resolution.

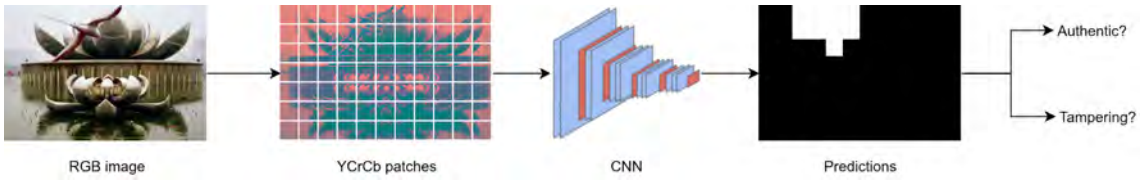


Figure 4.7: The entire framework. A RGB picture, initially, is separated into covering patches. Ultimately, linear stage is intended to confirm the predctions of the network and confirm a final decision on the verification of picture

4.7 The Whole Framework

A slider of size 64 is used group if a given image is not real, to take out coverage (step 32) from the image. Such fixes are performed through the revamped MBNV2 network to test validation after being changed to the RGB color channel. A while later, a post-preparation process is to record neighborhood data from scores to pick names compared to patches. Accept that there are k neighbors in fix p0, which is rated by the network s(p0), indicated as pi(i = 1; k). Thus, it is possible to assess its dependability as follows.

On the off chance that the dependability surpasses an threshold (0 1), name for the patch p0 is positive, except if, the mark is negative. The entire system portrayed in Fig. 1.

Input	Layer	t	c	n	s
224^2 x 3	Conv2d 3x3	-	32	1	2
112^2 x 32	bottleneck	1	16	1	1
112^2 x 16	bottleneck	6	24	2	2
56^2 x 24	bottleneck	6	32	3	2
28^2 x 32	bottleneck	6	64	4	2
14^2 x 64	bottleneck	6	96	3	1
14^2 x 96	bottleneck	6	160	3	2
7^2 x 160	bottleneck	6	320	1	1
7^2 x 320	Conv2d 1x1	-	1280	1	1
7^2 x 1280	avgpool	-	-	1	-
1x 1280	Conv2d 1x1	-	-	-	-

Figure 4.8: Original MobileNetV2 Architecture

Input	Layer	t	c	n	s
64^2 x 3	Conv2d 3x3	-	32	1	1
64^2 x 32	bottleneck	1	16	1	1
64^2 x 16	bottleneck	6	24	2	1
64^2 x 24	bottleneck	6	32	3	2
32^2 x 32	bottleneck	6	64	4	2
16^2 x 64	bottleneck	6	96	3	1
64^2 x 96	bottleneck	6	160	3	2
8^2 x 160	bottleneck	6	320	1	1
8^2 x 320	Conv2d 1x1	-	1280	1	1
8^2 x 1280	avgpool	-	-	1	-
1 x 1280	**Linear 1280x2**	-	-	-	-

Figure 4.9: Modified MobileNetV2 Architecture

$$Reliability = 1 / k + 1 \sum_{i=0}^{k} s(pi)$$

4.8 Metrics

To assess the model, some normal measurements are utilized. Four metrics are TP- True Positive , TN - True Negative, FP - False Positive and FN - False Negative. Measurements processed follows.

$$Accuracy = TP + TN / TP + TN + FP + FN$$

$$Precision = TP / TP + FP$$

$$Recall = TP / TP + FN$$

$$Fscore = 2 * Precision * Recall / Precision + Recall$$

Accuracy learns how precise the model performs among these measurements. Be that as it may, due to the recognition of inconsistency , accuracy is not sufficient infer the program's quality because class with the number of tests is overpower class with less than one. In addition, Precision and Recall are used in this way in order to resolve in these types of problems. There is a balance between precision and recall, depending on any individual application. Individuals often misuse the F score as a solitary reward for two metrics to speak up for this agreement. The greater these characteristics, the greater the totality of the four dimensions, the better the show of the model.

We may follow their trustworthy ones from data inside file names of forged images. We may achieve ground truth by conducting deduction, filtering, and thresholding. The white regions depict distorted artifacts in terrestrial worlds, while the dark regions are special.

4.9 Data Preparation

We use the dataset CASIA2 in [39] to prepare and analyze our model. This dataset includes more than 12,000 images as seen, of which there are about 7,500 valid images and about 5,000 manipulated images. In particular, tampered images are controlled by different types of techniques from genuine images (e.g., copy movement, splicing, relative shift, obscuring edges of tampering). Despite the fact that the data cannot show ground truth to show which fragments are created in altered

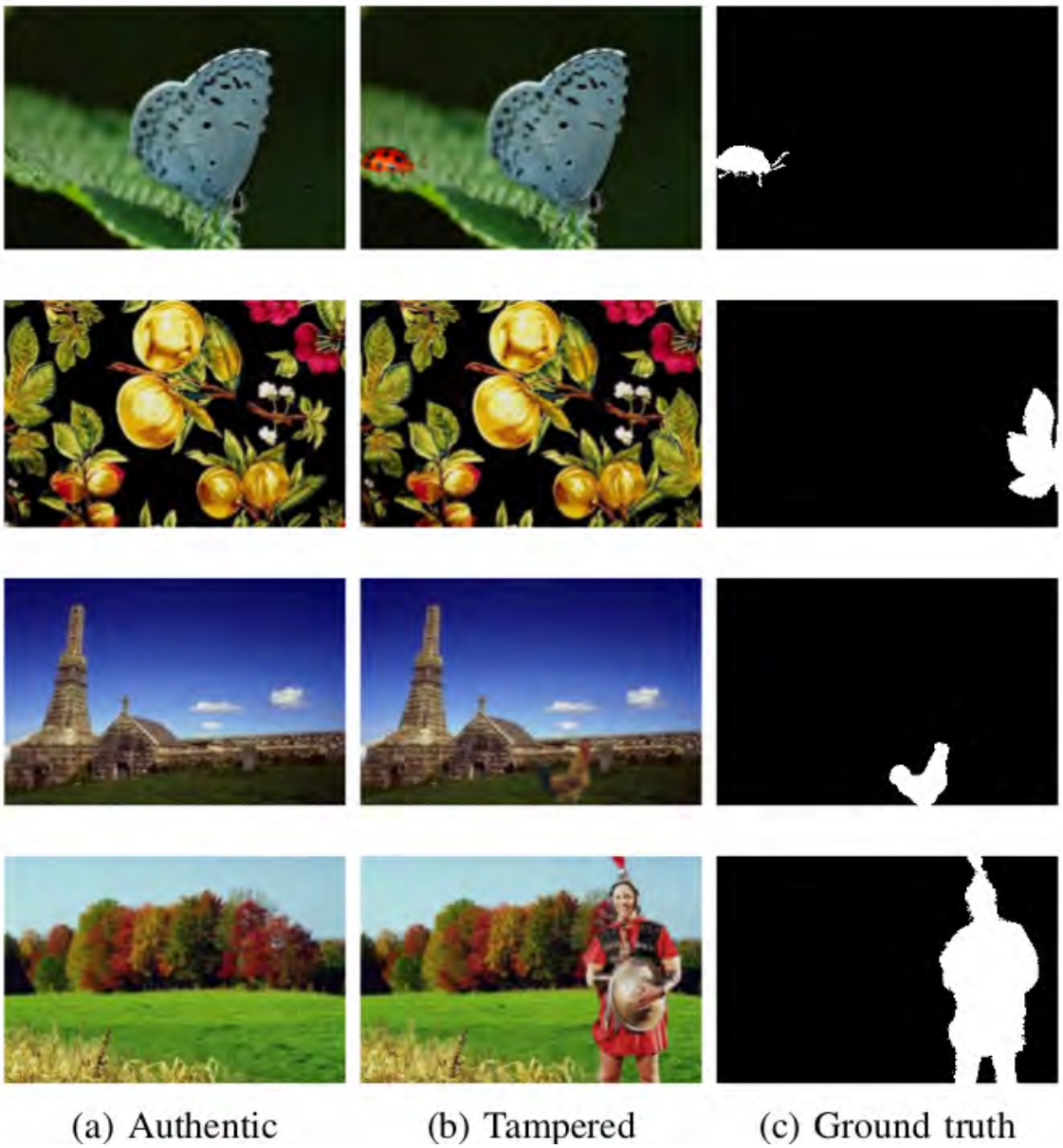


Figure 4.10: Differences between forged and authentic images

photos, we may assume this by removing a fake image and its real one based on the faking technique data construct fake photo within its document name.The analysis is isolated and calculated within a limit at that point in order to obtain the forgery guide. Fig. Fig. 2 offers some maps of forgery acquired from their genuine and fake photos. Consequently, we assert these maps of forgery as facts. We prepare data for training much like research in the aftermath of researching the ground truth. Since our model 's contribution is of dimension 64x64, we produce a lot of size 64 image patches that are cut from photos. Patches are haphazardly of non-tampered images wherever they are to be trimmed. By and by, forged patches inside pictures are trimmed at explicit locations. We use slider over the reality of the earth, firmly. The sliding is achieved with a 64 kernel size and an 8 phase difference. If the forged region level of a window lies in limit from 0.3 to 0.5, the slider is used to trim faked fragments. Finally, a dataset of 329914 authentic and 341365 altered fragments is completed, with 6238 valid and 3888 tampered photos in place. In particular, the training set has 90 percent, leaving 10 percent for the approval. This dataset is used to prepare and approve the model. In addition, the remainder is for research, with 1253 valid and 766 invalid photographs. Dataset rundowns in Table III.

Dataset	Authentic	Tampered
Training	255031 patches	278411 patches
Validating	31785 patches	33569 patches
Testing	1258 images	754 images

Figure 4.11: Dataset Summary

4.10 Training

A total of 277051 negative fragments and 298155 positive fragments for program testing are in the training process. Both of them are the size of 64 patches. To prevent over fitting the training package, magnification techniques are applied, including random turns in the magnet and rotation in the angle -30 to 30 range. Until expanding to the limit of unity, the images are then changed to the YCrCb color channel. Next, it performs normalization:

$$I\,(c)\,norm \;=\; I\,(c) \;-\; m\,(c)/\,d\,(c)$$

Where the picture is I, c Y, Cr, Cb represents the color channel, m (c) [0.485, 0.456,

0.406] and d (c) [0.229, 0.224, 0.225] are comparable the normal color channel deviation values are the same. From a set of training data, both vectors are calculated. In addition, a further validation dataset containing 30,863 authentic and 33,210 manipulative samples will be established to validate the general status of the model. The photos in this data not for training the metrics of the architecture, but are used to calculate span, learning rate, and decay in weight. Using the method above, these photos are not modified.

$$L = -1\,CCX - 1\,i = 0\,yi\,Ln\,(\hat{}yi) + (1 - yi)\,LN\,(1 - yi)$$

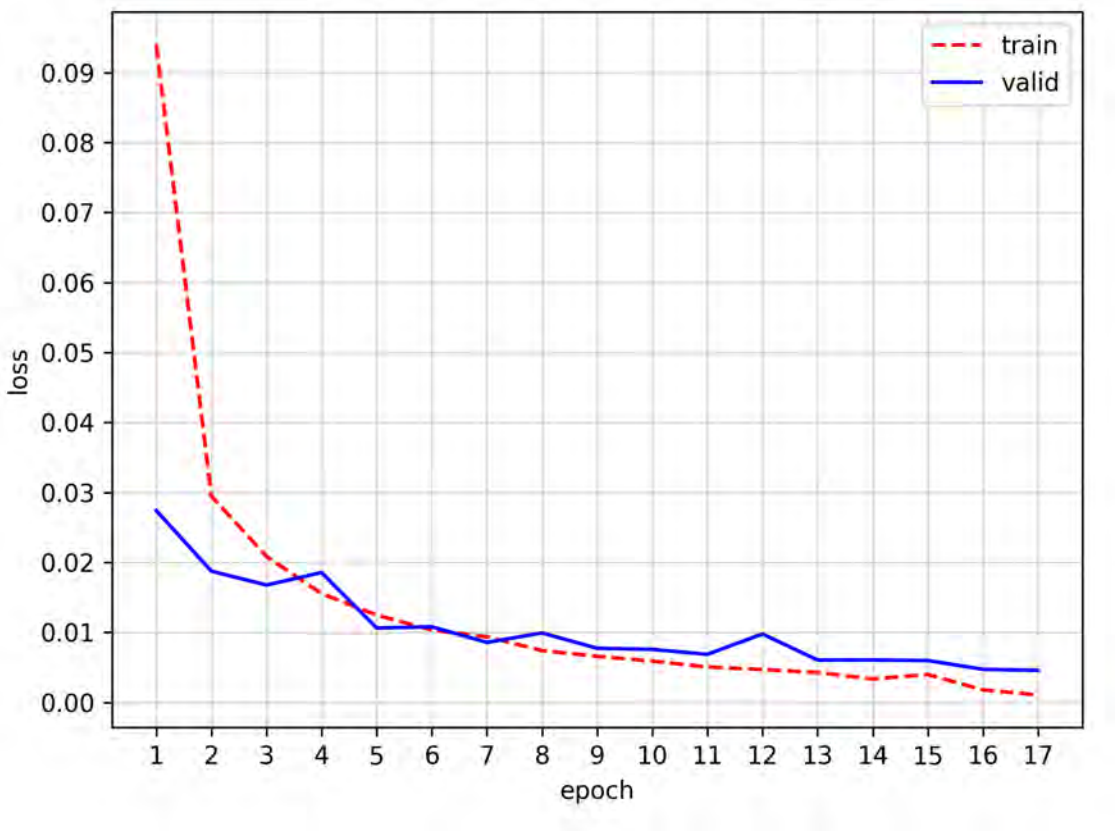


Figure 4.12: Loss and Accuracy during the process of preparation. Notice that these metrics are computed as levels of patch

4.11 Testing

In this section, we used 1253 authentic and 766 images to test the trained model, the set used is equal to 1/6th the size of the CASIA 2 database. Patches of 64 bit are sent to the network and where the scores are determined by neighborhood information of the patches. If the entire image is negative, then if an overall black image

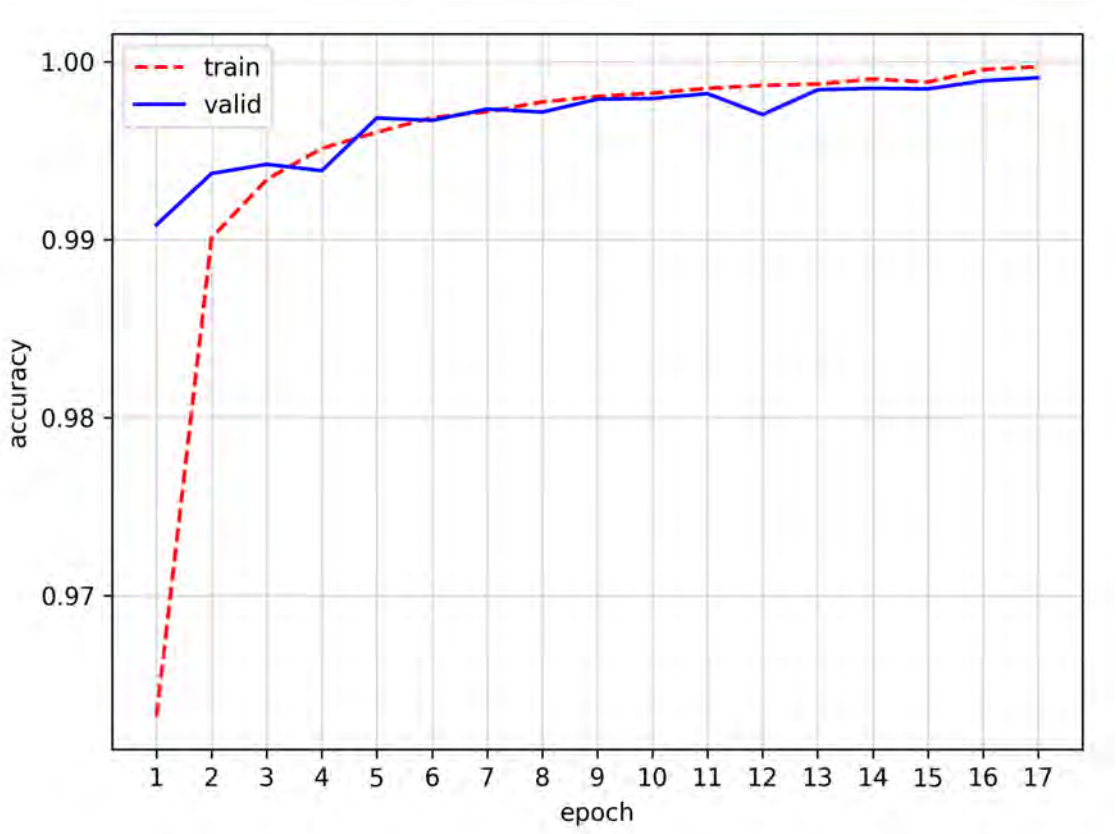


Figure 4.13: Precision during the training stage. Notice that these metrics are computed as levels of patch

is seen with the absence of positive patches, the photo is original, but if the case is such that there is a positive patch, the image will be considered to be tampered.

In addition, we also perform an exhaustive review of product designs to demonstrate the aspect enhances the model's final presentation. We characterize six arrangements accompanied by MobileNetV2, referred to as MBN2, as the nucleus, to make sense of this. The widely familiar RGB and YCrCb, which are more susceptible to tampering, are two color channels. In addition, three architectures of MobileNetV2 and VGG16 are considered for comparison. MobileNetV2 is the main engineering prepared without any planning, the next one is MobileNetV2 with pre-prepared ImageNet loads, the third is a revamped MobileNetV2 prepared from the ground up and VGG16 is the fourth one used.

Table 4 indicates the implications of the association between models. Models prepared with YCrCb images work better, as can be seen.

The modified MobileNetV2 shape is the best, followed by MobileNetV2 pre-trained by ImageNet, which is more, the rest is MobileNetV2 prepared. It is quite clear right off the bat that the model prepared without any planning does not meet the standards set by the model with ImageNet-pretrained loads. This is because of very prepared channels for the large image dataset scope, so these channels can easily adapt to our dataset. In addition, considering the fact that MobileNetV2 is prepared with RGB images on the ImageNet dataset, convolutionary channels are found out how to produce highlights from bottom-level, edges, corners, to elevated levels such as objects , for example.

Model	Accuracy	Precision	Recall	F-score
MBN2-RGB	77.50%	85.51%	65.21%	77.75%
MBN2-YCrCb	82.14%	65.10%	77.58%	72.01%
MBN2-pre-RGB	75.69%	57.75%	68.77%	64.78%
MBN2-pre-YCrCb	82.06%	72.50%	82.20%	75.70%
MBN2-mod-RGB	90.08%	94.48%	82.85%	85.14%
MBN2-mod-YCrCb	**93.15%**	**96.26%**	**91.63%**	**90.83%**

Figure 4.14: Performance Comparison

Model	Number of parameters	Model Size (MiB)	Inference Time
MBN2-RGB	2,235,434	23.05	5.7
MBN2-YCrCb	2,235,434	23.05	5.7
MBN2-pre-RGB	2,235,434	23.05	5.7
MBN2-pre-YCrCb	2,235,434	23.05	5.7
MBN2-mod-RGB	2,286,674	116.25	6.5
MBN2-mod-YCrCb	2,286,674	116.25	6.5

Figure 4.15: Computation Comparison

Chapter 5

Result Analysis

5.1 Comparison Between VGG16 and MobileNetV2

As a result of the experiments, we obtained that for the model trained in the zero-stage and even for the pre-trained, the proposed solution based on CNN has substantially greater accuracy. The following table presents the results produced in terms of splicing recognition by the model.

Method	Accuracy,%	Precision,%	Recall,%
Markovian rake transform [16]	75.74	-	-
Image Chroma [17]	86.8	-	-
Markov Chain [18]	85.6	-	-
DCT Coefficients Analysis [19]	80.1	-	-
The proposed approach	86.4	85.0	88.1
The proposed approached (fine tuned)	87.8	87.1	86.8

Figure 5.1: Detecting splicing forgery using CASIA Dataset

Table 4 shows the effect of examination between models. Models prepared with RGB images are, as can be seen, more regrettable than those prepared with RGB pictures.Subtle altering information is painstakingly darkened in the RGB architec-

Data	Accuracy,%	Precision,%	Recall,%
Initial	86.4	84	81.1
Compressed(Q=90)	57.1	72.1	42.3
Compressed(Q=80)	56.3	70.4	55.1

Figure 5.2: Results genarated by CNN based on compression quality

ture as people monitor images by programming with the purpose of perceiving these tasks in an RGB channel is truly unforgiving.

Model	Accuracy	Precision	Recall	F-score
MBN2-RGB	77.50%	85.51%	65.21%	77.75%
MBN2-YCrCb	82.14%	65.10%	77.58%	72.01%
MBN2-pre-RGB	75.69%	57.75%	68.77%	64.78%
MBN2-pre-YCrCb	82.06%	72.50%	82.20%	75.70%
MBN2-mod-RGB	90.08%	94.48%	82.85%	85.14%
MBN2-mod-YCrCb	**93.15%**	**96.26%**	**91.63%**	**90.83%**

Figure 5.3: Performance Comparison

Model	Number of parameters	Model Size (MiB)	Inference Time
MBN2-RGB	2,235,434	23.05	5.7
MBN2-YCrCb	2,235,434	23.05	5.7
MBN2-pre-RGB	2,235,434	23.05	5.7
MBN2-pre-YCrCb	2,235,434	23.05	5.7
MBN2-mod-RGB	2,286,674	116.25	6.5
MBN2-mod-YCrCb	2,286,674	116.25	6.5

Figure 5.4: Computation Comparison

Chapter 6

Conclusion

6.1 Conclusion

A procedure is described in this paper recognize forged images. The system relies on rapid and lesser calculations costs of MBNV2[40]. In any case, we adjust the organization in a manner that the spatial target of time layers right remains unchanged, enabling the architecture to learn rich highlights from input befor those enrich highlights from upper layers.In addition, far-reaching experiments are aimed at contrasting model arrangements, which demonstrate the adequacy of the updated adaptation of MobileNetV2. The last test result shows that the presentation of the modified organization on the CASIA2 data set is fair with an accuracy of 93.15%.

6.2 Future Plans

The study discusses a new method of recognizing digital images using CNN MobileNetV2 for artificial distortions. The samples obtained demonstrate a bigger quality of image recognition (92.2 percent accuracy for the fine-tuned model. A detailed comparison with other methods of splicing detection and recognition of distorted areas is planned on horizon. We also decide to equate the given solution to the CNN models Inception-v4 and Resnet-50.

Reference

[1] Amit, Dutta, Kumar. (2019, March 20). CNN Based Image Forgery Detection Using Pre-trained AlexNet Model. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355402

[2] Zhang, Y. (2016, April 7). Image Region Forgery Detection: A Deep Learning Approach. Retrievedfrom https://www.semanticscholar.org/paper/Image-Region-Forgery-Detection%3A-A-Deep-Learning-Zhang-Goh/613c63818e03bbb56cbcef1d3f0061d0d37e5966

[3] J. Chen, X. Kang, Y. Liu and Z. J. Wang, "Median Filtering Forensics Based on Convolutional Neural Networks," in IEEE Signal Processing Letters, vol. 22, no. 11, pp. 1849-1853, Nov. 2015.

[4] Sudiatmika, I. B. K. (2019, April 1). Image forgery detection using error level analysis and deep learning — Sudiatmika — TELKOMNIKA (Telecommunication Computing Electronics and Control). Retrieved from http://journal.uad.ac.id/index.php/TELKOMNIKA/article/view/8976

[5] Abdalla, Y. E. (2020, April 7). Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network. Retrieved from https://www.semanticscholar.org/paper/Copy-Move-Forgery-Detection-and-Localization-Using-Abdalla-Iqbal/745e6e22232cc6c190013d928b5acfb16039f8ee

[6] Kuznetsov, Andrey. (2019). Digital image forgery detection using a deep learning approach. Journal of Physics: Conference Series. 1368. 032028. 10.1088/1742-6596/1368/3/032028.

[7] M. T. H. Majumder and A. B. M. Alim Al Islam, "A Tale of a Deep Learning Approach to Image Forgery Detection," 2018 5th International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 2018, pp. 1-9.

[8] Wang, Xinyi Wang, He Niu, Shaozhang Zhang, Jiwei. (2019). Detection and localization of image forgeries using improved mask regional convolutional neural network. Mathematical Biosciences and Engineering. 16. 4581-4593. 10.3934/mbe.2019229.

[9] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, 2016, pp. 1-6.

[10] P. Rota, E. Sangineto, V. Conotter and C. Pramerdorfer, "Bad teacher or unruly student: Can deep learning say something in Image Forensics analysis?," 2016 23rd International Conference on Pattern Recognition (ICPR), Cancun, 2016, pp. 2503-2508.

[11] R. R. K. and M. Wilscy, "Pretrained Convolutional Neural Networks as Feature Extractor for Image Splicing Detection," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, 2018, pp. 1-5.

[12] Hashmi, Mohammad Farukh Anand, Vijay Keskar, Avinas. (2014). Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform. AASRI Procedia. 9. 84–91. 10.1016/j.aasri.2014.09.015.

[13] CASIA Tampered Image Detection Evaluation Database 2010 URL: http://forensics. idealtest.org/casiav2

[14] Simonyan K, Zisserman A 2014 Very deep convolutional networks for large-scale image recognition arXiv preprint arXiv:1409.1556

[15] Abdalla, Y. (2019, September 21). Image Forgery Detection Based on Deep Transfer Learning — European Journal of Electrical Engineering and Computer Science. Retrieved from https://www.ejece.org/index.php/ejece/article/view/125

[16] Sutthiwan P, Shi Y Q, Zhao H, Ng T-T and Su W 2011 Markovian rake transform for digital image tampering detection Transactions on data hiding and multimedia security VI 1-17

[17] Wang W, Dong J and Tan T 2009 Effective image splicing detection based on image chroma ICIP. IEEE 1257-1260

[18] Wang W, Dong J and Tan T 2010 Image tampering detection based on stationary distribution of markov chain ICIP. IEEE 2101-2104

[19] Lin Z, He J, Tang X and Tang C-K 2009 Fast, automatic and fine grained tampered jpeg image detection via DCT coefficient analysis Pattern Recognition 42(11) 2492-2501

[20] X. Pan and S. Lyu, "Region duplication detection using image feature matching", IEEE Transactions on Information Forensics and Security,vol. 5, no.4, ISSN: 1556-6013, pp. 857-867, 2010.

[21] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G.Serra, "A siftbased forensic method for copy move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol.6, no. 3, ISSN: 1556-6013, pp. 1099-1110, 2011.

[22] P. Kakar, N. Sudha, "Exposing post processed copy-paste forgeries through transform-invariant feature", IEEE Transactions on Information Forensics and Security, vol. 7,no.3, ISSN: 1556-6013, pp. 1018-1028,June 2012.

[23] D.G. Lowe, "Object recognition from local scale-invariant features",Proceedings

of the 7th IEEE International Conference on Compute rVision, Kerkyra, Greece, Sept. 1999.

[24] H. Bay, A. Ess, T. Tuytelaars, L. V. Gool, "Speeded-Up Robust Features (SURF)",Proceedings of the 9th European conference on Computer Vision, Graz, Austria, May 2006.

[25] Z. Lin, J. He, X. Tang, K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", Pattern Recognition, vol. 42, no. 11, ISSN: 0031-3203, pp. 2492-2501, January 2009.

[26] W. Wang, J. Dong, T. Tan, "Exploring DCT coefficient quantization effects for local tampering detection", IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, ISSN: 1556-6013, pp. 1653-1666,October 2014.

[27] L. Chen, T. Hsu, "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection", IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, ISSN:1556-6013, pp. 396-406, June 2011

[28] M. Bashar, K. Noda, N. Ohnishi, K. Mori, "Exploring Duplicated Regions in Natural Images", IEEE Transactions on Image Processing, ISSN:1057-7149, March 25, 2010.

[29] T.L. Tien, T.H. Ngoc, T.H. Kha, M. Luong, "Zernike Moment Based Approach for Detecting Duplicated Image Regions by a Modified Method to Reduce Geometrical and Numerical Errors", Book Chapter as Lecture Note in Computer Science (LNCS) by Springer, SEPA-ICCSA 2015, Banff, Canada, June 2015.

[30] Z. Zhang, G. Wang, Y. Bian, Z. Yu, "A novel model for splicing detection", 2010 IEEE Fifth International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA), Changsha, China,September 2010.

[31] O. Muratov, D.T.D Nguyen, G. Boato, F.G.B.D. Natale, "Saliency detection as a support for image forensics", 2012 5th International Symposium on Communications, Control and Signal Processing, Rome,Italy, June 2012.

[32] X. Pan, X. Zhang, S. Lyu, "Exposing image forgery with blind noise estimation", MMSec 11 Proceedings of the thirteenth ACM multimedia workshop on Multimedia and security, New York, USA, September 2011.

[33] J. Fridrich, and J. Kodovsk, "Rich models for steganalysis of digital images", IEEE Transactions on Information Forensics and Security, vol.7, no. 3, pp. 868-882, June 2012.

[34] J. Goh, V.L.L. Thing, "A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection", International Journal of Electronic Security and Digital Forensics, ISSN: 1751-911X, vol. 7, no.1, pp. 76-104, March

2015.

[35] Y. Zhang, J. Goh, L. Win, V. Thing, “Image Region Forgery Detection: A Deep Learning Approach”, Proceedings of the Singapore Cyber-Security Conference, Singapore, 2016, ISBN: 978-1-61499-616-3.

[36] Rao Yuan, Ni Jiangqun, “A deep learning approach to detection of splicing and copy-move forgeries in images”, IEEE International Workshopzon Information Forensics and Security (WIFS), Abu Dhabi-United Arab Emirates, 2016, ISBN: 978-1-5090-1139-1.

[37] J. Bunk, J.H. Bappy, T.M. Mohammed, L. Nataraj, A. Flenner, B.S. Manjunath, S. Chandrasekaran, A.K.R. Chowdhury, and L. Peterson, “Detection and Localization of Image Forgeries using Resampling Features and Deep Learning”, IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, USA, July 2017

[38] T.L. Tien, H.P. Xuan, T.N. Chinh, T.D. Tieu, “Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model”, International Journal of Machine Learning and Computing, ISSN: 2010-3700, vol. 9, no. 2, pp. 181-188, April 2019.

[39] J. Dong and W. Wang, “Casia tampering detection dataset”, 2011.

[40] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, L.-C. Chen, “MobileNetV2: Inverted Residuals and Linear Bottlenecks”, https://arxiv.org/ abs/1801.04381, January 2018.